REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-18 are pending in the present application, Claims 1, 4, 5, 8, 10, and 12-18 having been amended, and Claims 2, 3, and 7 having been canceled without prejudice or disclaimer. Support for the amendments to Claims 1, 4, 5, 8, 10, and 12-18 is found, for example, in original Claims 1-18. Thus, no new matter is added.

In the outstanding Office Action, Claims 5, 6, 12, and 13 were objected to; Claims 1-18 were rejected under 35 U.S.C. §112, second paragraph; and Claims 1-9, 11, and 14-18 were rejected under 35 U.S.C. §102(b) as anticipated by Delayaye et al. (U.S. Patent No. 4,751,733, hereinafter Delayaye); and Claims 10, 12, and 13 were rejected under 35 U.S.C. §103(a) as unpatentable over Delayaye in view of Matsui et al. (U.S. Patent No. 6,201,869, hereinafter Matsui).

With respect to the objections to Claims 5, 6, 12, and 13, Claims 5, 6, 12, and 13 are amended to remove "a" as suggested in the outstanding Office Action.

With respect to the objection to Claims 5 and 6 as duplicates of each other, Applicants respectfully submit that the amendments to Claims 5 and 6 overcome the objection. Claim 5 recites, *inter alia*, "input bit terminals of a second nonlinear transformation unit," and Claim 6 recites, *inter alia*, "input bit terminals of more than one of the second nonlinear transformation units." Thus, Applicants respectfully submit that Claims 5 and 6 have different scope.

In response to the rejection of Claims 1-18 under 35 U.S.C. §112, second paragraph, Claims 1-18 are amended, without adding new matter, to address the deficiencies identified in the outstanding Office Action. Accordingly, this ground for rejection is believed to have been overcome. If, however, the Examiner disagrees, the Examiner is invited to telephone

the undersigned who will be happy to work with the Examiner in a joint effort to derive mutually satisfactory claim language.

In a non-limiting embodiment of the claimed invention, nested (recursive) SPN encryption includes a combination of local randomization (lower-level diffusion) and diffusion over a block width (higher-level diffusion). As shown in Fig. 1, each of the parallel nonlinear transformation modules (extended S-boxes) 2 in each stage executes local, lower-level diffusion. Diffusion module (a higher-level MDS) 3 executes broad, high-level diffusion over the block width. Each nonlinear transformation module 3 is constructed by alternately arranging nonlinear transformation modules (S-boxes) and diffusion modules (lower-level MDS). That is, in the nested SPN structure, lower-level SPN structures (two stages of SPN structures) are recursively embedded in S-box portions of the normal SPN structure.[1]

In the non-limiting embodiment of the claimed invention, the security of the nested (recursive) SPN encryption against SQUARE attack is higher than SQUARE encryption/Rijndael encryption because of randomizing by the higher-level MDS diffusion layer provided between S-boxes (between the second-half S-boxes of the preceding (or the last) extended S-box and the first-half S-boxes of the succeeding (or the first) extended S-box).[2]

SQUARE attack on SPN encryption follows a procedure of inputting 256 patterns (Λ set) that satisfies conditions: (1) variable bytes take 256 patterns, and (2) other bytes are fixed and searching for a key for which the bit sum for 256 patterns becomes zero, thereby estimating the key.[3]

---

[1] Specification, page 10, lines 23-26, and page 11, lines 15-24.
[2] Specification, page 47, line 24 to page 48, line 6.
[3] Specification, page 48, lines 7-12.

The security against SQUARE attack is improved by adding given conditions to the combination in the higher-level MDS (the combination relationship among input and output bits of the higher-level MDS or the interconnect relationship among operational paths). The given conditions double or multiply all or part of the differential paths (operational paths between the first half of S-boxes of the preceding extended S-box and the first half S-boxes of the succeeding extended S-box). Thus, a high avalanche effect is achieved and the number of stages that are subject to SQUARE attack are reduced.[4]

The higher-level MDS, for the non-limiting embodiment of the claimed invention, is arranged based on the following criteria:

(1) any selected one of the S-boxes (a total of 16 S-boxes in Figs. 30-35) in the first-half of the preceding extended S-box 103 and any selected one of the S-boxes (a total of 16 S-boxes in Figs. 30-35) in the first-half of the succeeding extended S-box 103 are interconnected (coupled) by two or more paths; and

(2) the inverse transform or inverse function of linear diffusion performed by the higher-level MDS (i.e. the higher-level MDS on the decryption circuit side) exists and it also satisfies the same condition as in (1).[5]

As shown in Fig. 35, for a non-limiting embodiment of the claimed invention, an S-box 1001 (in the first half of the preceding extended S-box) and an S-box in the first-half of the succeeding extended S-box 1002 (in the first-half of the succeeding extended S-box) are interconnected by two paths indicated by bold lines. Other S-boxes are interconnected by two to four paths. The doubling or multiplying of all or part of the differential paths allows one bit to be transmitted via at least two routes, and increases the avalanche effect.

[4] Specification, page 48, lines 13-26.
[5] Specification, page 52, line 18 to page 53, line 14.

In contrast with the conventional SQUARE encryption/Rijndael encryption shown in Fig. 36, an S-box 1001 in the first-half of the preceding extended S-box and an S-box 1002 in the first-half of the succeeding extended S-box are interconnected by only one path. Therefore, the avalanche effect in the conventional technique is low.

Turning now to the rejection of independent Claim 1 as anticipated by Delayaye, Applicants respectfully submit that the amendment to Claim 1 overcomes the rejection. Claim 1 is amended to recite, *inter alia*, "wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths." Delayaye does not teach or suggest at least this element of amended Claim 1.

Figs. 5 and 6 of Delayaye show wiring diagrams used to perform permutation operations. As shown in Figs. 5 and 6, each bit is only connected to one other bit via one path.

Furthermore, Matsui does not teach or suggest "wherein the first units and the second unit are configured to connect at least one input bit terminal of the first units to one input bit terminal of the corresponding first unit in the succeeding encryption section via at least two paths."

Matsui only describes a nonlinear transformer 131 including a Galois Field inverse circuit 152.[6] Matsui does not teach or suggest nested (recursive) SPN encryption including a combination of local randomization (lower-level diffusion) and diffusion over the block width (higher-level diffusion).

In view of the above noted distinctions, Applicants respectfully submit that Claim 1 patentably distinguishes over Delayaye and Matsui, alone or in combination. In addition, independent Claims 4 and 12-18 recite elements similar to the elements of Claim 1. Thus,

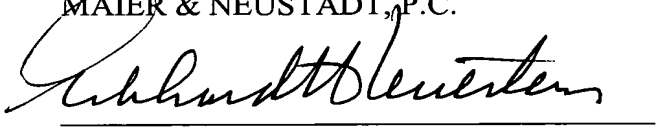
[6] Matsui, Fig. 2.

Applicants respectfully submit that Claims 4, and 12-18 (and Claims 5, 6, 8 and 9-11) patentably distinguish over Delayaye and Matsui, alone or in combination.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)
I:\ATTY\JW\210580US\210580US_AM DUE 8-28-05.DOC